IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF: (I) THE PREMISES KNOWN AS RINDGE, NEW HAMPSHIRE; (II) THE PREMISES KNOWN AS RINDGE, NEW HAMPSHIRE; (III) THE PERSON OF MICHAEL J. DAVINI; AND (IV) THE PERSON OF MICHELE DAVINI	Case No. 20-mj- 223-01-AJ

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Special Agent Todd Donnelly, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for four anticipatory search warrants authorizing law enforcement to search (i) the premises known as Rindge, New Hampshire (hereinafter the "Subject Residence"); (ii) the premises known as , Rindge, New Hampshire (hereinafter the "Lake House"), collectively the "PREMISES"; (iii) the person of Michael J. DAVINI (hereafter "DAVINI"); and (iv) the person of Michele DAVINI, further described in Attachments A-1, A-2, A-3, and A-4, for the things described in Attachment B.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18 of the United

States Code. I also am a "federal law enforcement officer" within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

3. I am a Special Agent with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and have been employed in that capacity since June 2003. Prior to my employment as a Special Agent, I worked as a Police Officer in the State of Maine from 1994 to 2003. My formal training for these positions took place at the Federal Law Enforcement Training Center in Glynco, Georgia, and the Maine Criminal Justice Academy. During my career, I have conducted or participated in a wide array of investigations involving the illegal manufacture, smuggling and distribution of contraband, to include control substances and counterfeit merchandise.

4. I am presently assigned to the HSI Manchester, New Hampshire, Resident Field Office. Included in my current assignment is to serve on the Joint Terrorism Task Force (JTTF) in the New Hampshire Office of the Federal Bureau of Investigation ("FBI"), which I have done since 2009. My duties and responsibilities as a Special Agent include, among other things, conducting criminal investigations of individuals who have violated Federal criminal laws listed in Title 18, Title 19 and Title 21 of the United States Code.

5. The information set forth in this affidavit is based on my own investigation; information from other law enforcement officers; information provided by businesses relating to this investigation; physical surveillance; queries conducted of law enforcement databases; public records; and information gained from my training and experience.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts set forth in this affidavit, there is probable cause to believe that Michael J. DAVINI committed the offenses of Unlawful Possession of a Punch Die, 21 U.S.C. § 331(i)(2) and ; 21 U.S.C. § 843(a)(5); Smuggling Goods into the United States, 18 U.S.C. § 545; and Unlawful Importation of Drug Paraphernalia, 21 U.S.C. § 863(a)(3). There is also probable cause to believe that DAVINI uses the Subject Residence and/or the Lake House in furtherance of these criminal violations, and that DAVINI may carry on his person a cellular telephone, a laptop computer, a notebook, or other records or electronic devices that are used in and contain evidence of these crimes. Accordingly, there is cause to believe that searches of DAVINI, the Subject Residence and the Lake House will lead to the seizure of evidence, fruits, and instrumentalities of the aforementioned crimes, as well as to the identification of accomplices and co-conspirators who may be engaged in the commission of these crimes and related violations of the law.

RELEVANT STATUTES

8. 21 U.S.C. § 331(i)(2), provides in relevant part:

> The following acts and the causing thereof are prohibited: . . . Making, selling, disposing of, or keeping in possession, control, or custody, or concealing any punch, die, plate, stone, or other thing designed to print, imprint, or reproduce the trademark, trade name, or other identifying mark, imprint, or device of another or any likeness of any of the foregoing upon any drug or container or labeling thereof so as to render such drug a counterfeit drug.

The term "counterfeit drug" means "a drug which, or the container or labeling of which, without authorization, bears the trademark, trade name, or other identifying mark, imprint, or device, or any likeness thereof, of a drug manufacturer, processor, packer, or distributor other than the person or persons who in fact manufactured, processed, packed, or distributed such drug and which thereby falsely purports or is represented to be the product of, or to have been packed or

distributed by, such other drug manufacturer, processor, packer, or distributor." 21 USC § 321(g)(2).

9. 21 U.S.C. § 843(a)(5) provides in relevant part:

> It shall be unlawful for any person knowingly or intentionally . . . to make, distribute, or possess any punch, die, plate, stone, or other thing designed to print, imprint, or reproduce the trademark, trade name, or other identifying mark, imprint, or device of another or any likeness of any of the foregoing upon any drug or container or labeling thereof so as to render such drug a counterfeit substance . . . .

The term "counterfeit substance" means "a controlled substance which, or the container or labeling of which, without authorization, bears the trademark, trade name, or other identifying mark, imprint, number, or device, or any likeness thereof, of a manufacturer, distributor, or dispenser other than the person or persons who in fact manufactured, distributed, or dispensed such substance and which thereby falsely purports or is represented to be the product of, or to have been distributed by, such other manufacturer, distributor, or dispenser." 21 U.S.C. § 802(7).

10. 18 U.S.C. § 545 provides in relevant part:

> Whoever fraudulently or knowingly imports or brings into the United States, any merchandise contrary to law, or receives, conceals, buys, sells, or in any manner facilitates the transportation, concealment, or sale of such merchandise after importation, knowing the same to have been imported or brought into the United States contrary to law . . . [s]hall be fined under this title or imprisoned not more than 20 years, or both.

Based on discussions with other law enforcement agents, I know that the importation of an item that falls within the ambit of 21 U.S.C. § 331(i)(2) is a triggering event for 18 U.S.C. § 545. In other words, importing merchandise that is in violation of 21 U.S.C. § 331(i)(2) satisfies the "contrary to law requirement" of 18 U.S.C. § 545.

11. 21 U.S.C. § 863(a)(3) provides that "[i]t is unlawful for any person . . . to import or export drug paraphernalia." The term "drug paraphernalia" means, among other things, "any equipment, product, or material of any kind which is primarily intended or designed for use in manufacturing, compounding, converting, concealing, [or] producing . . . a controlled substance, possession of which is unlawful under this subchapter [Subchapter I of Title 21]." 21 U.S.C. § 863(d).

PROBABLE CAUSE

12. On November 13, 2020, United States Customs and Border Protection ("CBP") Boston Targeting Unit, encountered an international DHL Express Shipment (the "Target Package") identified by Waybill No. 4132, coming from China and destined for in Rindge, New Hampshire (the Lake House). CBP determined that the Target Package was addressed to "Kujo Lafiette," a name that was later determined to be fictitious.

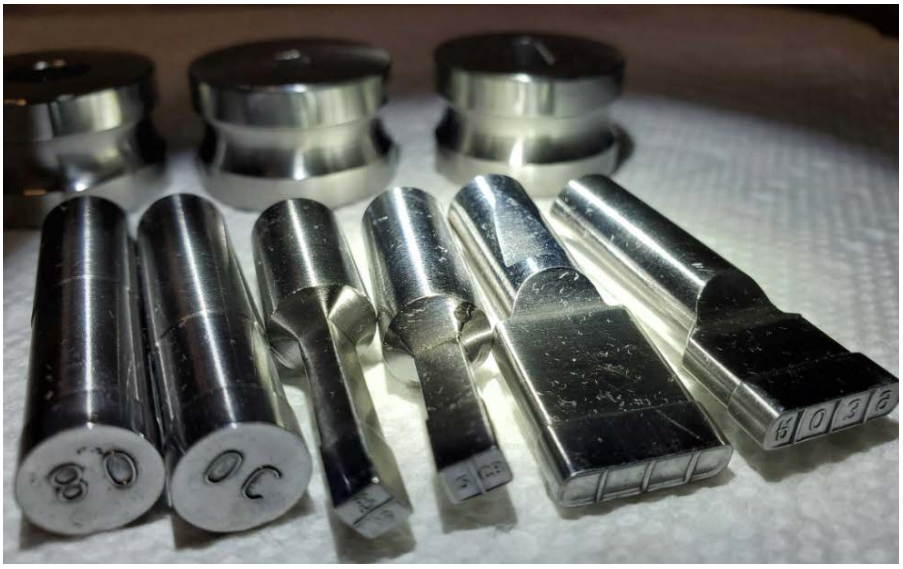
13. The contents of an international packages arriving to the United States from abroad is described in the manifest. Based upon my training and experience, packages that are sent to the United States that contain illegal contraband, are always manifested as something other than what the package truly contains. I learned from JST Logistics, which does business as DHL throughout New England, that the Target Package was manifested as auto parts.

14. The invoice associated with the parcel provided "Receiver Details," including the telephone number 3517. The "contact name" on the invoice is "kujo lafiette," the addressee of the Target Package. An HSI analyst conducted queries in multiple databases for the person Kujo Lafiette and found no evidence that a person with that name exists.

15. CBP opened the Target Package and found nine pieces that made up three pill press die kits, which are used for stamping pharmaceutical grade pills. Pill dies and parts are subject to the Controlled Substance ACT and regulated by the Drug Enforcement Administration. 21 U.S.C. § 843(a)(5).

16. According to a joint project by the National Association of Boards of Pharmacy, National Association of Drug Diversion Investigators, and The Partnership for Safe Medicines, "A pill press is a mechanical device used to compress powder into tablets of uniform size by running powder through a machine fitted with die molds that determine the shape and markings on the tablets. These machines were originally conceived as tools for pharmaceutical development and manufacturing and dietary supplement makers, but drug traffickers use them to make counterfeit pills laced with fentanyl, MDMA tablets, and other illicit drugs. Pill presses vary in capacity from "desktop machines" that can make approximately 1,800 pills an hour, to massive industrial machines that can produce 1.6 million pills per hour." The suggestion that pill presses are readily available through international sources online is consistent with my knowledge, training and experience as an HSI agent provided with the authority to enforce Custom Duties as defined by Title 19 of the U.S. Code.

17. As described below, CBP determined the pill dies to be prohibited drug paraphernalia subject to seizure under 21 U.S.C. § 863(a)(3) and 19 U.S.C. § 1595a(c)(2)(A) because their features contained, "the trademark, trade name, or other identifying marks, imprints or device of another or any likeness of any of the foregoing upon any drug or container or labeling thereof so as to render such drug a counterfeit substance;" a violation of 21 U.S.C. § 843(a)(5).



18. In making this determination, CBP compared the imprint and shape of the dies through a web-based "Pill Identifier" tool at Drugs.com. Through this process, CBP positively identified two of the press dies—that, respectively, imprint "OC"/"80" and "R 0 3 9"—as being replicas for producing OxyContin 80 mg and Alprazolam 2 mg. Specifically, the Drugs.com Pill Identifier states that a "[p]ill with imprint OC 80 is Green, Round and has been identified as OxyContin 80 mg" and lists the "Labeler/Supplier" as "Purdue Pharma LP." The Pill Identifier also states that a "[p]ill with imprint R 0 3 9 is Yellow, Rectangle and has been identified as Alprazolam 2 mg" and lists the "Labeler/Supplier" as "Actavis."

19. The third die set, pictured above, imprints 2 CB on a pill. The Pill Identifier did not identify the pill associated with this die set. Based upon the imprint of the die set, coupled with intelligence data, CBP came to the conclusion that the die was made for producing "2C-B" (2,5-dimethoxy-4-bromophenethylamine), a psychedelic drug commonly referred to as "Pink Cocaine", "Tucibi" and "Tusi." A DHS Information Bulletin describes 2C-B as a stimulant, empathogen, hallucinogen and psychedelic compound that draws comparisons to LSD and MDMA.

20. On November 18, 2020, CBP notified the HSI office in Manchester, NH, of the seized Target Package. HSI advised that they would accept delivery of the item for further investigation. On November 24, 2020, HSI received the Target Package at the HSI office in Manchester, New Hampshire, where it was subsequently entered into evidence.

PROPERTIES – SUBJECT RESIDENCE & LAKE HOUSE

21. Property records pertaining to the consignee address (the delivery address) associated with the Target Package (Rindge, New Hampshire 03461; aka, the Lake House), indicate that the property at that address is owned by Michele DAVINI (DOB: , wife to Michael DAVINI Property records of the Lake House show that Michael DAVINI sold the property to his wife in 2015. The DAVINI's were married on August 31, 2013, and by all indications they remain married today.

22. New Hampshire Department of Motor Vehicle records provide that both Michele and Michael DAVINI hold a valid New Hampshire driver license with an address of Rindge, New Hampshire (the Subject Residence). Michele DAVINI's license was issued October 28, 2020, while Michael DAVINI's license was issued November 16, 2020.

23. New Hampshire Department of Motor Vehicle records also provide that Michael and Michele DAVINI currently have five vehicles and two utility trailers registered between the two of them at the Subject Residence.

24. Surveillance conducted on November 24, 2020 revealed that the Lake House is located directly across the street from the Subject Residence Three vehicles were in the driveway of the Subject Residence at the time of surveillance, two of which were registered to Michele DAVINI and one registered to Michael DAVINI.

25. At the time of surveillance, the Lake House appeared unoccupied. The Lake House is located on a small, partially wooded parcel of land that resembles an island and contains a footbridge that connects the land to the shoreline, which abuts The driveway leading towards the Lake House ends where the footbridge begins; however, a path of gravel runs parallel with the footbridge, which would allow for a vehicle to cross over to the island property. Based on the height of the footbridge and the surrounding waterline, it appeared as though water levels could rise high enough to prevent anyone from driving across, leaving the footbridge as the only means for crossing. The Lake House is a small, gray one-story building, approximately 1,000 square feet is size, which has the appearance of being a summer home.

26. Located down the road from the Lake House and Subject Residence, where intersects with are a series of individual mailboxes. One of the mailboxes is colored blue with the number "52" written on the front and "DAVINI" written on the side. Another mailbox is grey in color with written on the front and "DAVINI" written on the side.

27. The Subject Residence appears to be a newly built construction, possibly within the past year or two. It is a two-story home that is partially surrounded by a black chain link fence, which is approximately four feet high. The residence is white in color and has an attached two-car garage. The garage has a full dormer on one side, giving it the appearance of a great room over the 2 bays, which is attached to the main home. The property is contained on a parcel of land that is mostly open, yet sandwiched between and The driveway and front of the home faces while the back of the home faces and has clear view towards the Lake House

28. While initial review of property records pertaining to the ownership of the Subject Residence was inconclusive, all evidence obtained thus far would support that Michael and Michele DAVINI are both residing at this address.

MICHAEL DAVINI BACKGROUND

29. A criminal history query with NCIC revealed that on November 4, 2019, Michael DAVINI was criminally charged in Massachusetts with "Medical Assistance Fraud by Provider". DAVINI's residence associated with the charge is Rindge, New Hampshire (the Lake House).

30. Further research into DAVINI's criminal history, through open source data and information provided by the Attorney General's Office for the Commonwealth of Massachusetts, revealed that on October 12, 2016, DAVINI, who was the owner and operator of Rite Way LLC, along with three of his managers, were indicted in a $19 million dollar scheme that defrauded the Commonwealth's Medicaid program known as MassHealth. Rite Way was a MassHealth provider of non-emergency wheelchair van services that primarily operated to provide

MassHealth members with transportation to and from methadone clinics. The indictment alleged that between 2011 and 2015, DAVINI through his operation of Rite Way, submitted claims for payment to MassHealth for transportation services that were either never provided or not provided as claimed. As a result, DAVINI was indicted on multiple felony counts of Medicaid Fraud, charging him with Medicaid false claims, larceny over $250 and Medicaid kickbacks.

31. In 2018, DAVINI was indicted on three additional felony counts of Money Laundering in relation to the healthcare fraud scheme. According to the Commonwealth's Sentencing Memorandum, these charges came about after DAVINI, "abruptly transferred $3 million, plus real estate holdings, to his wife in order to disguise the nature, location, source, ownership or control of the property derived from criminal activity."

32. On October 24, 2019, DAVINI plead guilty in Worcester Superior Court to charges in connection with fraudulently billing millions of dollars in false claims to the Commonwealth's Medicaid Program. On November 4, 2019, DAVINI was sentenced to 1 year in the House of Correction (2 ½ years suspended), followed by 5 years of probation. He was also ordered to pay $4.2 million dollars in restitution. Records indicate that DAVINI was released from prison in May of 2020 and remains on probation.

TELEPHONIC CONNECTIONS

33. On November 23, 2020, HSI served Verizon Wireless with a Title 21 DHS administrative subpoena for records pertaining to telephone number 3517—the telephone number found on the invoice within the Target Package. As discussed, the "contact name" on the invoice is "kujo lafiette," the addressee of the Target Package.

34. The subpoena requested Verizon records for a limited period of one month from October 19, 2020 through November 20, 2020. On November 24, 2020, HSI received the subpoena results. The records showed no subscriber for the phone number and instead said "Please forward to reseller: TracFone Wireless, Inc." While TracFone references a specific mobile telecommunications company, it is often synonymous with the term "drop phone" or "burner phone", based on the difficulty in tracking the subscriber associated with telephone number. Based upon my training and experience, these types of phone are regularly used during the course of criminal activity.

35. The subpoenaed records also show that telephone number 3517 had been in contact with telephone numbers associated with Michael and Michele DAVINI. A review of the telephone tolls for 3517, between the dates of October 19, 2020 and November 20, 2020, revealed there were 24 calls between this number and 8814, a number that is known to be associated with DAVINI. According to a search for records conducted on December 2, 2020, through a law enforcement database, 8814 is an active wireless number belonging to DAVINI.

36. A review of the telephone tolls for 3517 between the dates of October 19, 2020 and November 20, 2020, revealed there were 5 text messages between this number and 1004, a number that is known to belong to Michele DAVINI. Multiple sources, including her U.S. passport application in 2014, indicates 1004 belongs to Michele DAVINI. Open source records have also directly associated this number with out of Fitzwilliam, New Hampshire, a company that is owned and operated by Michele DAVINI.

PRIOR SHIPMENTS

37. Records provided by CBP revealed that at least four prior international shipments were made to the Lake House address in 2020, three of which took place in October 2020, and had the same fictitious consignee as the Target Package, Kujo Lafiette. The fourth shipment was sent in March 2020, which listed Michele DAVINI as the consignee. The most recent of these packages delivered to the Lake House took place on October 26, 2020. This package has been identified by DHL Express Shipments Waybill No 5216.

38. JST Logistics, which does business as DHL throughout New England, provides delivery services for DHL by delivering their international packages. According to JST Logistics, all DHL packages require a signature from the consignee before they are delivered, unless the consignee inputs an "ODD" (On Demand Delivery) into the system, which gives the driver permission to leave the package at the front door. An ODD can also provide the driver with specific instructions if they are requesting the package be delivered somewhere other than the front door.

39. According to JST Logistics, all of the information pertaining to the package associated with Waybill No. 5216, was the same as the Target Package, including the shipper and consignee. The only difference between the two packages is that Waybill No. 5216 was five pounds heavier than the Target Package. JST Logistics confirmed that an ODD was entered into the system for the parcel associated with Waybill No. 5216. The driver who delivered this package confirmed the he remembered doing so because there were instructions to leave it near the footbridge (which leads over to the Lake House). JST has also confirmed that there is an ODD is in the system for the Target Package.

40. Records HSI received from CBP also revealed prior international shipments associated with Michael and Michele DAVINI. The last two shipments associated with Michael DAVINI took place in 2012 and 2014. Since this time 11 additional international shipments were made to Michele DAVINI listed as the consignee. Of the 11 shipments, 4 have taken place in 2020. Of the 4 shipments, 3 were delivered to the Subject Residence, while one was delivered to the Lake House.

DRUG TRAFFICKERS' AND THE USE OF RESIDENCES

41. Based upon my training and experience, I am familiar with illegal drug distribution, including the methods used by individuals to store, transport and distribute illegal narcotics, drug paraphernalia and the proceeds of drug distribution. I am also familiar with such individuals' use of common carriers like Federal Express, UPS and DHL to transport and distribute illegal narcotics and drug paraphernalia.

42. I know from my training and experience that drug distribution can involve the local, interstate, and international movement of illegal narcotics to distributors and co-conspirators; and the movement of the proceeds of drug trafficking among multiple participants, including suppliers, customers, distributors, and money launderers.

43. I know from my training and experience that drug traffickers will use common carriers because of its speed and reliability; and the availability of telephone and internet tracking.

44. In my training and experience, I have acquired specialized knowledge regarding drug traffickers' use of residences and other homes to store and process narcotics for

distribution. I have also been involved in the execution of search warrants at the homes of individuals involved in narcotics distribution.

45. Based upon my training and experience, I am aware that it is generally a common practice for drug traffickers to store their drug inventory, drug paraphernalia, drug proceeds, and drug records either in their own homes or in the own residences, businesses, and vehicles of relatives, trusted associates, or others. The reason that drug dealers use the homes of others to store drugs is because drug traffickers know that selling narcotics is illegal and can subject traffickers to lengthy prison sentences. As a result, drug traffickers often attempt to distance themselves from the drugs that they are selling by either having them delivered and/or storing them at the homes of friends/associates, which is typically a residence or commercial location that is often being used by drug traffickers to hold narcotics or package them for distribution.

46. Based upon my training and experience, as well as the training and experience of other law enforcement agents I have worked with, I am aware that it is generally a common practice for drug traffickers to store drug-related paraphernalia in their residences for longer periods of time. Further, it is generally a common practice for drug traffickers to maintain in their residence's records relating to their drug trafficking activities. Because drug traffickers in many instances will "front" (that is, sell on consignment) controlled substances to their clients, or alternatively, will be "fronted" controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep "pay and owe" records to show balances due for drugs sold in the past ("pay") and for payments expected ("owe") as to the trafficker's suppliers and the trafficker's dealers. Additionally, drug traffickers

must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their drug trafficking business. I am also aware that drug traffickers often maintain such documents related to their drug trafficking activities at their residences for an extended period of time, regardless of whether they are physically in possession of drugs on the premises.

47. Based upon my training and experience, as well as the training and experience of other law enforcement agents I have worked with, I am also aware that it is generally a common practice for traffickers to conceal at their residences (or inside the residences or businesses or vehicles of relatives or trusted associates) large sums of money, either the proceeds from drug sales or monies to be used to purchase controlled substances. In this connection, drug traffickers typically make use of wire transfers, cashier's checks, and money orders to pay for controlled substances. Evidence of such financial transactions and records relating to income and expenditures of money and wealth in connection with drug trafficking would also typically be maintained in residences.

48. Based upon my training and experience, as well as the training and experience of other law enforcement agents I have worked with, I am also aware that drug traffickers generally try to hide cash and sensitive documents related to their drug trafficking activities in safes or other containers so that other individuals who are at their residence do not discover these materials.

49. Based upon my training and experience, as well as the training and experience of other law enforcement agents I have worked with, I know that most drug dealers regularly communicate using cellular telephones.

50. Persons who receive drugs through parcels often have done so in the past and are prepared to do so in the future and keep mailing labels and air bills both used and unused. Additionally, such drug traffickers often send the proceeds of their drug sales via overnight delivery to their suppliers in order to pay for a continuing supply of drugs. Further, based on my training and experience, I am aware that evidence of occupancy, residency, rental and/or ownership of the premises is relevant to the prosecution of the offense which this affidavit establishes.

51. Accordingly, based on the above-stated information, and upon my experience and the experience of other law enforcement officers who have participated in the execution of numerous search warrants at the residences of drug-traffickers, I am aware that the following kinds of drug-related evidence have typically been recovered from the search of the drug-traffickers' residences:

a. controlled substances;

b. paraphernalia for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;

c. books, records, receipts, notes, ledgers, and other papers relating to the distribution of controlled substances;

d. personal books, and papers containing names, addresses, telephone numbers, and other contact or identification data relating to the distribution of controlled substances;

e. cash, currency, and records relating to controlled substances income and expenditures of money and wealth, such as money orders, wire transfers, cashier's checks and receipts, bank statements, passbooks, checkbooks, and check registers, as well as precious metals such as gold and silver, and precious gems such as diamonds, and currency counting machines;

f. documents indicating travel in interstate and foreign commerce such as travel itineraries, plane tickets, boarding passes, motel and hotel receipts, passports and visas, credit card receipts, and telephone bills;

g. cellular telephones;

h. blank air bills or labels for overnight deliveries and receipts for mailing of shipments;

i. items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the subject premises. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

TECHNICAL TERMS

52. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a

series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

53. Based on my experience and training, I know that individuals who arrange for contraband to be shipped and/or imported most often use phones, computers, or other electronic devices to arrange for such shipment or importation, and to arrange payment for the item(s) being shipped or imported. I also know that communications between buyers in one country and

sellers in another country frequently occur via electronic communications (for example, email or application-based messaging).

54. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

55. *Probable cause*. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

56. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under

investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

57. *Necessity of seizing or copying entire computers or storage media*. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge

that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

58. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

59. Because several people share the PREMISES as residences, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

THE ANTICIPATORY SEARCH WARRANT

60. As discussed below, I seek an anticipatory search warrant for the Subject Residence and Lake House upon successful delivery of the Target Package.

61. Within the timeframe specified by the search warrant, JST Logistics, doing business as DHL, will deliver Target Package to the Lake House, unless instructed otherwise by the consignee.

62. It has been my experience that packages containing contraband, when delivered by way of controlled delivery, will either be transported to another location or opened shortly after delivery is made. In light of these circumstances, there may be practical difficulties in obtaining access to the United States Magistrate Judge in a timely fashion. Therefore, I request that anticipatory search warrants for the premises known and described as the Subject Residence and Lake House and the person of Michael J. DAVINI (see Attachments A-1, A-2, A-3) be issued today with its execution contingent upon fulfillment of the following:

a. On or about December 10, 2020, a driver with JST Logistics doing business as DHL, will deliver the Target Package to the Lake House (believed to be unoccupied) by leaving it outside of the front door or another designated area as instructed by the consignee.

b. Agents will conduct surveillance of the Lake House and Subject Residence prior to, during and after the delivery is made. Once an agent observes the Target Package enter into the Lake House or Subject Residence, agents will then execute the search warrants within the time period authorized. If the Target Package is not retrieved and brought inside one of the two premises, then the anticipatory

search warrants will not be executed, unless the contingency in subparagraph (c) below occurs.

c. In the event that the Target Package is retrieved but not brought to either residence, the investigating agents will follow the package and confront anyone who is in possession of it. If the package is taken into a vehicle, which then departs the area, a traffic stop will be conducted and the driver confronted. If either Michael or Michele DAVINI are identified as possessing the Target Package, then the anticipatory warrants on said persons will be executed. If only this contingency occurs, the anticipatory warrants to search the Lake House and Subject Residence will not be executed.

CONCLUSION

63. This affidavit supports probable cause for three anticipatory warrant to search (i) the premises known as Rindge, New Hampshire (hereinafter the "Subject Residence"); (ii) the premises known as Rindge, New Hampshire (hereinafter the "Lake House"), collectively the "PREMISES"; and (iii) the person of Michael J. DAVINI, and (iv) the person of Michele DAVINI, further described in Attachments A-1, A-2, A-3, and A-4, for the things described in Attachment B

REQUEST FOR SEALING

64. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and

information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

/s/ Todd Donnelly
Todd Donnelly
Special Agent
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Dec 9, 2020

/s/ Andrea K. Johnstone
Hon. Andrea K. Johnstone
United States Magistrate Judge

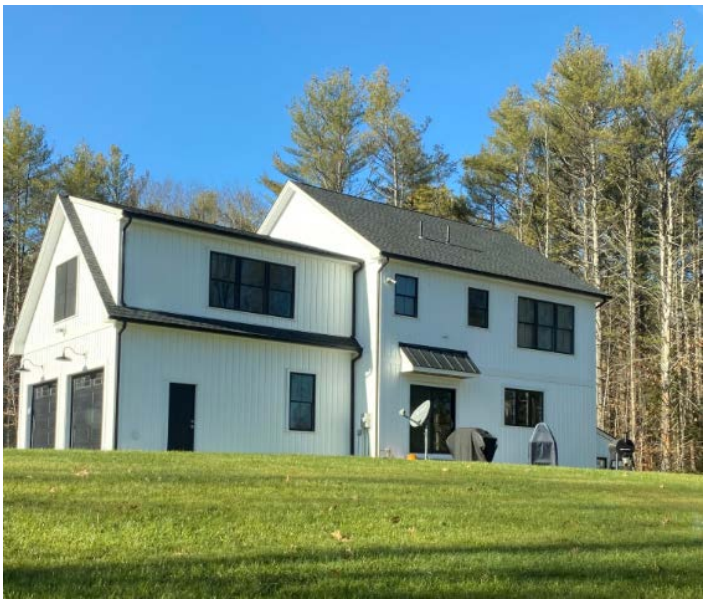
Time: 4:32 PM, Dec 9, 2020

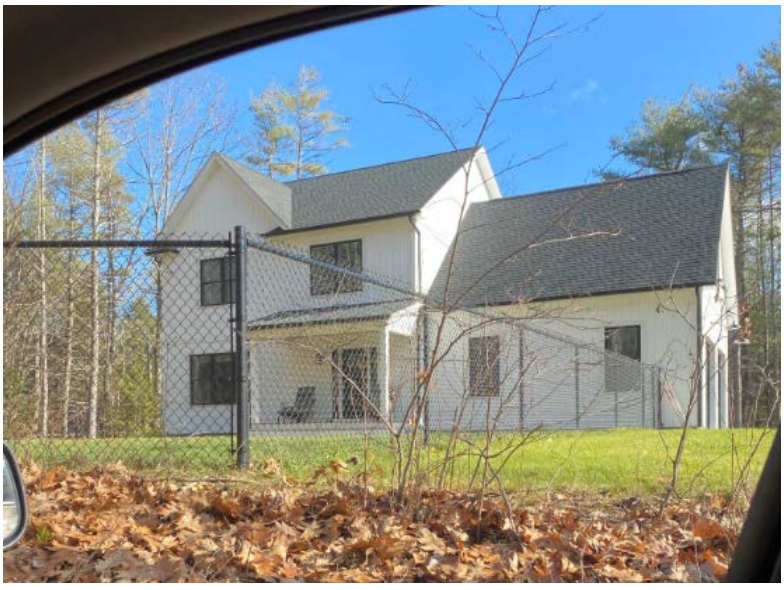
ATTACHMENT A-1

Property to be searched

The property to be searched is Rindge, New Hampshire (the "Subject Residence"). The Subject Residence, pictured below, has the appearance of a newly built construction that may have been built within the past year or two. It is a 2-story home that is partially surrounded by a black chain link fence, which is approximately 4 feet high. The residence is white in color and has an attached 2-car garage. The garage has a full dormer on one side, giving it the appearance of a great room over the 2 bays, which is attached to the main home. The property is contained on a parcel of land that is mostly open, yet surrounded by on one side and on the other. The driveway and front of the home faces while the back of the home faces which also has clear view towards a Lake House at Rindge, New Hampshire.

.

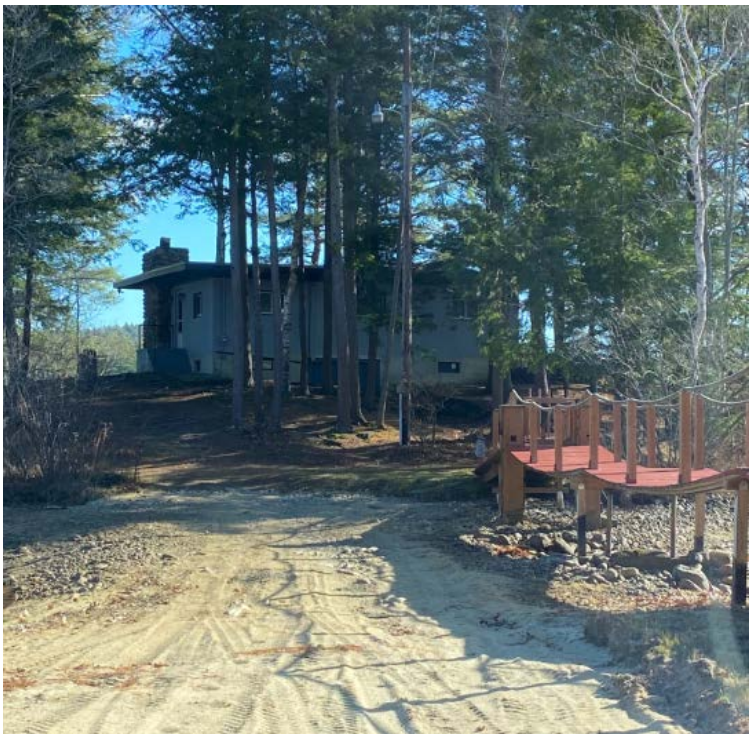


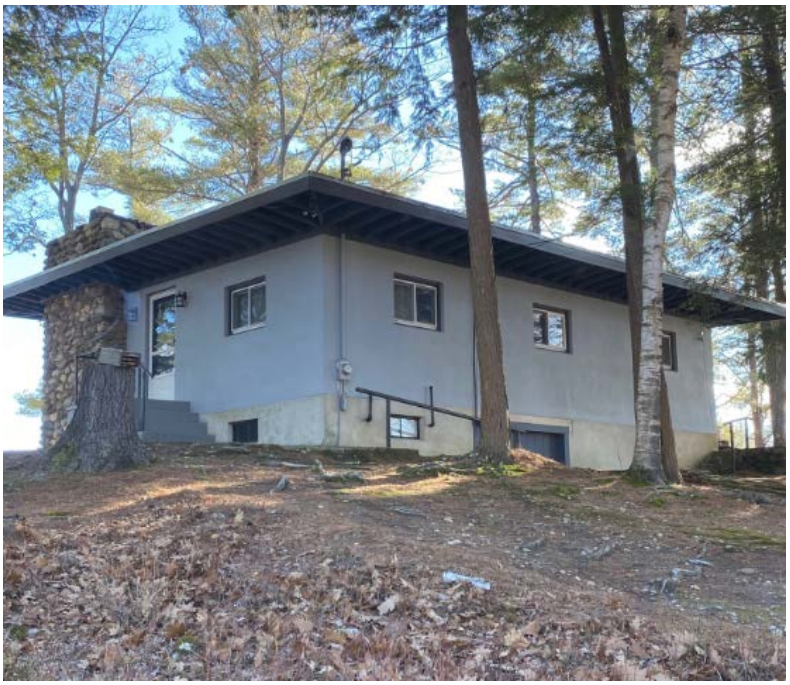


ATTACHMENT A-2

Property to be searched

The property to be searched is Rindge, New Hampshire (the "Lake House"). As pictured below, the Lake House is located on a small, partially wooded parcel of land that resembles an island and contains a footbridge that connects the land to the shoreline, which abuts The driveway leading towards the Lake House ends where the footbridge begins; however, a path of gravel runs parallel with the footbridge, which would allow for a vehicle to cross over to the island property. Based on the height of the footbridge and the surrounding waterline, it appeared as though water levels could rise high enough to prevent anyone from driving across, leaving the footbridge at the only means for crossing. The Lake House is a small, gray one-story building, approximately 1,000 square feet is size, which has the appearance of being a summer home.





ATTACHMENT A-3
Person to be searched

The person to be searched is Mr. Michael J. DAVINI, a U.S. Citizen with DOB and residing at Rindge, New Hampshire and/or Rindge, New Hampshire.

ATTACHMENT A-4
Person to be searched

The person to be searched is Ms. Michele DAVINI, a U.S. Citizen with DOB and residing at Rindge, New Hampshire and/or Rindge, New Hampshire.

ATTACHMENT B

Property to be seized

1. All records, fruits, evidence and/or instrumentalities relating to violations of 21 U.S.C. § 331(i)(2), 21 U.S.C. § 843(a)(5), 18 U.S.C. § 545, and 21 U.S.C. § 863(a)(3), those violations involving Michael J. DAVINI and Michele DAVINI, including:

a. Mobile Phone;

b. Storage Media;

c. Notebooks;

d. Credit and debit cards;

e. Personal effects or documents tending to establish property interest in the Subject Residence and Lake House, including, but not limited to, personal identification, driver's license, passports, vehicle registration certificates, birth certificates, deeds, bills, correspondence, utility and telephone bills, canceled envelopes, and rental/ purchase/lease agreements;

f. Records, communications, receipts, and information relating to the importation of pill press die kits, pill presses and or the illegal manufacturing of pills;

g. Counterfeit drugs, counterfeit substances, and controlled substances including OxyContin 80 mg, Alprazolam 2 mg, and 2C-B.

h. Ingredients and other paraphernalia used to manufacture counterfeit drugs and counterfeit substances;

i. Paraphernalia used and commonly associated with the possession and/or distribution of counterfeit substances and counterfeit drugs; and

j. Significant sums of U.S. Currency.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.